Velammal College of Engineering and Technology (Autonomous), Madurai

Department of Electronics and Communication Engineering

UNIT II MOBILE TELECOMMUNICATION SYSTEM

GSM: Architecture, Protocols, Connection Establishment, Frequency Allocation, Routing, Mobility Management, Security, GPRS, UMTS, Architecture.

CO2: Summarize the generations of telecommunication systems in wireless network.

Global System for Mobile Communications (GSM)

Architecture:

The architecture of GSM (Global System for Mobile Communications) is a carefully structured and layered system designed to provide reliable and efficient mobile communication. It is divided into three major subsystems, namely the **Mobile Station (MS)**, the **Base Station Subsystem (BSS)**, and the **Network Switching Subsystem (NSS)**. These subsystems are interconnected through standardized interfaces and work together to offer services such as voice communication, SMS, data transfer, mobility management, and roaming. The main objective of the GSM architecture is to separate radio-related functionalities from switching and subscriber-related functions, making the system easier to manage, scalable, and highly flexible.

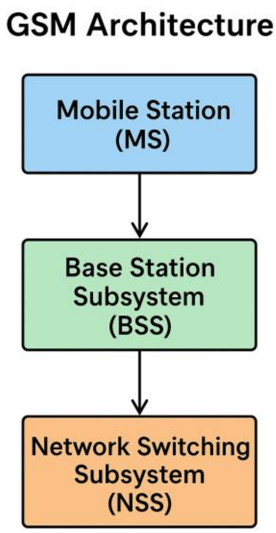


Fig: Architecture of GSM

The first component of the GSM architecture is the **Mobile Station (MS)**, which refers to the user's mobile device along with the SIM (Subscriber Identity Module) card. The mobile equipment contains all the hardware elements needed for communication, such as the transmitter, receiver, antenna, keypad, display, and battery. It also has a unique identifier called the IMEI (International Mobile Equipment Identity), used to identify the device. The SIM card stores essential subscriber information including the IMSI (International Mobile Subscriber Identity), authentication key (Ki), encrypted security parameters, and service details. The SIM enables user identity portability, meaning a user can insert their SIM into any GSM-compatible device and still access their subscribed services. The Mobile Station communicates with the network over radio channels and is responsible for handling functions such as signal measurement, encryption, authentication, and reporting signal strength to the BTS.

The MS communicates with the **Base Station Subsystem (BSS)**, which manages the radio interface between the network and the mobile device. The BSS consists of two important components: the Base Transceiver Station (BTS) and the Base Station Controller (BSC). The BTS is the radio equipment that handles transmission and reception of signals to and from the mobile devices. It contains antennas, transceivers, amplifiers, and signal processors. Each BTS defines the coverage area of a cell and broadcasts control information that mobile devices require to attach to the network. The BTS provides radio channels for voice, data, and signaling. Above the BTS is the BSC, which acts as its controller. The BSC manages several BTS units and is responsible for radio resource allocation, frequency management, handover control, power level adjustments, and traffic concentration. The BSC performs tasks that ensure efficient utilization of the radio spectrum and smooth transitions when a user moves from one cell to another. Together, the BTS and BSC form the entire radio access portion of the GSM network.

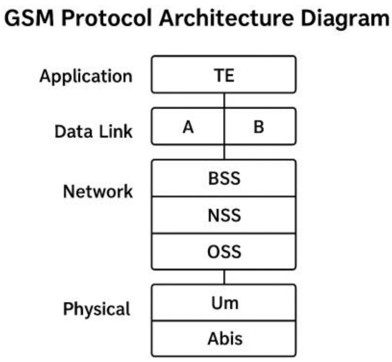
Beyond the BSS lies the **Network Switching Subsystem (NSS)**, which performs the core functions of switching, routing, subscriber management, and security. The central element of the NSS is the Mobile Switching Center (MSC). The MSC is responsible for setting up, maintaining, and terminating calls. It also handles routing of voice and data to other networks such as PSTN or ISDN. The MSC communicates with several important databases that help manage mobility and subscriber information. The **Home Location Register (HLR)** is a permanent database that stores long-term details about every subscriber, such as the IMSI, subscribed services, and current location (in terms of which VLR area the subscriber is registered in). The **Visitor Location Register (VLR)** is a temporary database that stores information about subscribers who are currently active or roaming within the MSC's service area. When a user moves into a new location area, the VLR updates the HLR to ensure accurate tracking of the subscriber.

Another important component of NSS is the **Authentication Center (AUC)**, which stores the secret authentication key (Ki) for each subscriber and generates authentication vectors to verify the identity of the user. This provides protection against fraud and unauthorized access. The **Equipment Identity Register (EIR)** is a database that stores information about mobile devices identified by their IMEI number and helps in blocking stolen, invalid, or unauthorized equipment from using the network. These NSS components work together with the MSC to ensure secure, reliable, and efficient connectivity.

Overall, the GSM architecture provides a highly modular and robust framework for mobile communication. By dividing the network into subsystems with specific responsibilities, radio communication handled by the BSS, subscriber and switching functions managed by the NSS, and user-based functions performed by the MS—the GSM system achieves high performance, excellent mobility support, international roaming capability, and strong security. This well-organized architecture is one of the primary reasons why GSM became the most widely adopted mobile communication standard worldwide.

<u>Protocols</u>

GSM uses a structured and layered set of protocols to manage communication between mobile stations, base stations, and the core network. These protocols are divided into several layers, where each layer is responsible for specific tasks such as signaling, mobility management, call control, encryption, and data transfer. GSM protocol architecture follows a modified OSI model and ensures that communication takes place in a secure, efficient, and organized manner. The entire GSM protocol stack is divided into three major protocol groups: **Radio Interface Protocols**, **Network Protocols**, and **Transport/Signalling Protocols**. Together, these protocols enable seamless voice calls, SMS transmission, location updates, authentication, and roaming.



The **Radio Interface Layer** forms the lowest part of the GSM protocol stack. It is responsible for managing the communication between the Mobile Station (MS) and the Base Transceiver Station (BTS). This layer deals with physical transmission of data, modulation, channel coding, interleaving, burst formatting, encryption, and frequency hopping. It includes the *Physical Layer (Layer 1)*, which handles the radio channel structure, time slots, frequency allocation, and power control. Above the physical layer is the **Data Link Layer**, also called the **LAPDm protocol**, which provides reliable data transfer over wireless channels. LAPDm is a modified version of LAPD used in ISDN, providing connection-oriented signalling with error detection and correction. It ensures that data frames exchanged between the MS and BTS are valid, properly sequenced, and acknowledged.

The next major group is the **Network Layer Protocols**, which operate mainly between the Base Station Controller (BSC), Mobile Switching Center (MSC), and other core network elements. The most important network-layer protocols are **RR (Radio Resource Management)**, **MM (Mobility Management)**, and **CC (Call Control)**. The **Radio Resource (RR) Protocol** manages the allocation and release of radio channels. It controls functions such as channel assignment, handover decisions, power regulation, timing advance, and measurement reporting. RR ensures that every mobile user receives a proper time slot or frequency without interference.

The **Mobility Management (MM) Protocol** handles the authentication of subscribers and maintains user location information. MM manages processes such as location update, IMEI checking, TMSI assignment, and roaming. It ensures that the network always knows which location area the subscriber belongs to so call routing becomes possible. The **Call Control (CC) Protocol** handles all procedures for call establishment, maintenance, and termination. CC follows the ISDN-based Q.931 signaling structure and manages both mobile-originated and mobile-terminated calls. It executes call setup messages, alerting signals, call clearance, and connection supervision.

In addition to these, GSM also includes **Supplementary Service Protocols** used for services such as call waiting, call forwarding, call barring, conference calling, and SMS-related signaling. These supplementary services share the same signaling link but operate using specific protocol groups defined in the GSM specifications.

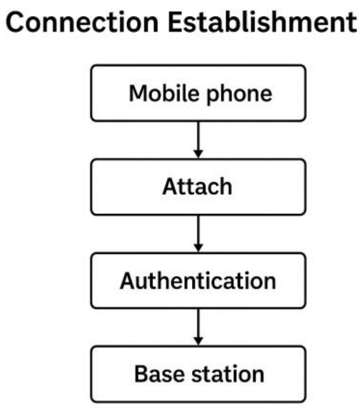
To support communication between the Base Station Subsystem (BSS) and the Network Switching Subsystem (NSS), GSM uses a dedicated signaling protocol called **BSSAP (Base Station System Application Part)**. BSSAP is divided into two components: **DTAP (Direct Transfer Application Part)** and **BSSMAP (BSS Management Application Part)**. DTAP transfers messages related to MM and CC between the MS and MSC. BSSMAP manages handovers, paging, channel assignment, and other BSS-level control functions. Both DTAP and BSSMAP operate on top of the **Signalling System No. 7 (SS7)** stack.

In the core network, GSM uses **SS7 signalling**, particularly the **MAP (Mobile Application Part)** protocol. MAP handles communication between HLR, VLR, MSC, SMSC, AUC, and EIR. It enables user authentication, location registration, roaming coordination, SMS delivery, and subscriber data exchange. MAP is essential for supporting global roaming because it connects GSM networks across different countries.

The entire GSM protocol stack is supported by reliable transport protocols such as **MTP (Message Transfer Part)** and **SCCP (Signalling Connection Control Part)** of the SS7 family. These provide routing, error detection, sequencing, and reliable delivery of signalling messages across the GSM network.

Connection Establishment:

Connection establishment in GSM is the process by which a mobile subscriber sets up a call with another user or receives a call from the network. It involves several coordinated procedures performed across the Mobile Station (MS), Base Station Subsystem (BSS), and Network Switching Subsystem (NSS). The entire process includes channel access, authentication, assignment of radio resources, call routing, and finally establishing a dedicated traffic channel. GSM uses a series of signaling exchanges to ensure secure and reliable setup of both mobile-originated and mobile-terminated calls.



When a **mobile-originated call** (user makes a call) occurs, the process begins when the subscriber dials a number and presses the call button. The Mobile Station first checks for the availability of an appropriate control channel. It typically uses the Random Access Channel (RACH) to send an access request to the network. The request contains information such as the mobile station's identity and the reason for access. The nearest Base Transceiver Station (BTS) receives the request and forwards it to the Base Station Controller (BSC) through the Base Station System. The BSC then assigns a Stand-alone Dedicated Control Channel (SDCCH) to the mobile device through an Access Grant Channel (AGCH). The SDCCH is used to perform critical signaling processes before a full traffic channel can be provided.

Once the mobile device receives the SDCCH assignment, the next step is **authentication**. The network verifies the identity of the subscriber using the authentication triplets generated by the Authentication Center (AUC). The AUC sends a random challenge (RAND) to the mobile station through the network. Using the secret key Ki stored in the SIM, the mobile station performs an encryption algorithm (A3) to compute a response (SRES), which it sends back to the network. If the response matches the expected value in the AUC, authentication is successful. Immediately after authentication, the network may initiate encryption activation using the A5 algorithm to secure the radio link and protect the call from eavesdropping.

Next, the **location and call setup signaling** phase begins. After authentication and encryption, the Mobility Management (MM) and Call Control (CC) protocols handle the exchange of messages required for the call setup. The mobile station sends a "call setup" request specifying the number dialed. The MSC checks the subscriber's profile in the HLR/VLR to confirm whether the user is allowed to make the requested call. If allowed, the MSC proceeds to establish a route toward the dialed number, either within the same network or toward the PSTN/ISDN.

Once routing is confirmed, the network begins the **traffic channel (TCH) assignment**. The BSC selects an available traffic channel, either a frequency/time slot combination (in GSM's TDMA structure), and instructs the BTS to allocate this channel to the mobile station. A "Channel Assignment" message is transmitted to the MS, directing it to tune to the assigned frequency and time slot. The mobile station synchronizes with the new channel and confirms successful switching by sending an acknowledgment. At this stage, the dedicated connection for voice or data has been established, and the speech or data transmission can begin.

In the case of a **mobile-terminated call** (incoming call), the process starts at the MSC. When a call arrives for a subscriber, the MSC queries the HLR to determine the user's current location area. The HLR responds with the address of the corresponding VLR. The MSC sends a paging request to all BTSs in that location area. All mobile stations in that area receive the paging message, but only the intended MS recognizes its Temporary Mobile Subscriber Identity (TMSI) or IMSI. The MS responds using the RACH, after which the BSC assigns an SDCCH just like in the mobile-originated case. Authentication, encryption, and call setup procedures follow in the same order. After confirmation, a traffic channel is assigned, and the MS rings, allowing the user to answer the call.

Frequency Allocation:

Frequency allocation in GSM refers to the systematic distribution and organization of radio frequency bands used for mobile communication. Since GSM operates on the principle of cellular reuse, proper allocation of frequencies ensures that each cell has sufficient channels for communication while minimizing interference between adjacent cells. GSM typically operates in standardized frequency bands such as 900 MHz, 1800 MHz, and 1900 MHz. In the GSM-900 band, the uplink frequency (from MS to BTS) ranges from **890–915 MHz**, and the downlink frequency (from BTS to MS) ranges from **935–960 MHz**, providing 25 MHz of paired spectrum. Similarly, GSM-1800 uses 1710–1785 MHz for uplink and 1805–1880 MHz for downlink.

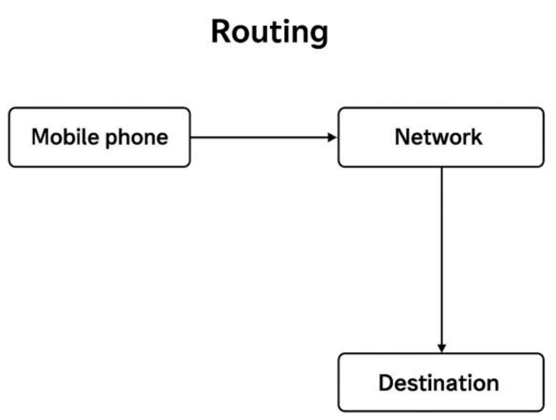
The available spectrum is divided into multiple carrier frequencies, each of which is separated by 200 kHz bandwidth. These carrier frequencies are used to support individual time slots within the TDMA frame structure. In each cell, one or more carriers are assigned depending on traffic demand. The role of the Base Station Controller (BSC) is crucial in determining how carriers are utilized within the BTS and how channels are assigned to users dynamically. To prevent interference, GSM uses frequency planning techniques such as frequency reuse, where the same set of frequencies can be repeated in nonadjacent cells. The reuse factor (usually 3, 4, 7, or higher) depends on the density of the traffic and the geographic nature of the region.

In addition to static planning, GSM employs dynamic frequency allocation wherein the BSC monitors channel quality and shifts traffic to frequencies that experience less interference. Other mechanisms, such as frequency hopping, also help in improving signal quality by rapidly changing carrier frequency at the mobile station and BTS. Overall, frequency allocation ensures efficient use of the limited radio spectrum, reduces co-channel and adjacent-channel interference, and supports smooth communication for millions of users simultaneously.

Routing

Routing in GSM refers to the process of determining how calls and messages travel from one user to another through the GSM network or external networks. A GSM call passes through several network components, including the MSC, HLR, VLR, and sometimes the PSTN or

ISDN. The routing procedure is different for mobile-originated (MO) and mobile-terminated (MT) calls. When a mobile user initiates a call, the Mobile Station first establishes a connection with the nearest BTS, which forwards the request to the BSC and then to the MSC. The MSC checks the subscriber profile in the VLR and determines if the call is allowed. If the destination user is within the same MSC area, the MSC performs internal routing and connects both users through the switching fabric.



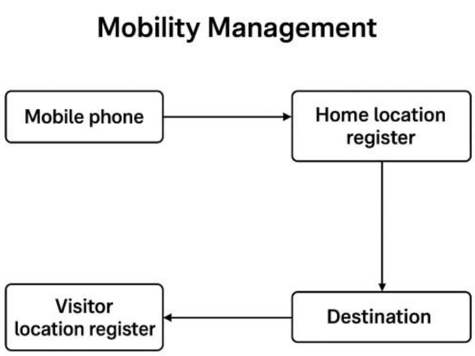
If the destination user belongs to another MSC or another network, the call is routed through the appropriate gateway. For calls leaving the GSM network, the **Gateway MSC (GMSC)** is responsible for interfacing with external networks like PSTN or ISDN. When an incoming call is received at the GMSC, the network queries the HLR to determine the location of the called subscriber. The HLR provides the address of the serving MSC/VLR, and the call is routed accordingly. The serving MSC then performs paging within the location area, sets up signaling through the BSS, and completes the call.

The routing process ensures that even if a user is roaming, the network can locate and route calls accurately. GSM routing also supports intelligent features such as supplementary services, number portability, SMS delivery, and handover routing. SMS routing, for instance, makes use of the SMSC (Short Message Service Center), which stores and forwards messages based on the recipient's availability. Thus, routing in GSM is an essential function that enables seamless connectivity across networks and geographic boundaries.

Mobility Management:

Mobility Management in GSM refers to all the procedures that allow subscribers to move freely within the network while maintaining continuous service. GSM supports both idle-mode and active-mode mobility. In idle mode, the system keeps track of the mobile's location at the granularity of a *Location Area (LA)*. Each location area contains several cells and is identified by a Location Area Identity (LAI). When a mobile station moves from one location area to another, it performs a **Location Update** procedure, informing the VLR and MSC about its new location. The VLR then updates the HLR accordingly, ensuring accurate routing of incoming calls.

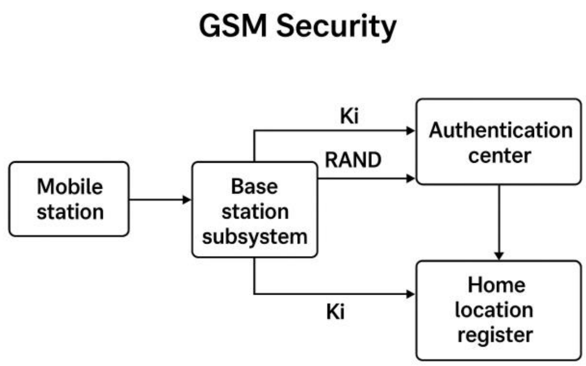
While the user is engaged in a call, mobility management handles **handover**. A handover occurs when the subscriber moves from one BTS coverage area to another and the signal quality drops below acceptable levels. The BSC continuously monitors signal strength and quality through measurement reports sent by the mobile station and BTS. Based on this information, the BSC or MSC decides when to perform a handover. GSM supports several types of handovers: **intra-cell**, **inter-cell**, **inter-BSC**, and **inter-MSC** handovers. During handover, the network assigns a new channel in the target cell, and the mobile station switches seamlessly without dropping the call.



Mobility Management also includes **authentication**, **ciphering**, and **temporary identity assignment**. When a subscriber registers in a new location area, the network may authenticate the user by verifying the SIM credentials through the AUC. To protect user identity, GSM assigns a Temporary Mobile Subscriber Identity (TMSI), preventing repeated transmission of the IMSI over the air. Ciphering keys are also updated to secure communication. The VLR and HLR keep track of the subscriber's status, location, and activity, ensuring that no matter where the user moves, the network always knows where to deliver calls and messages.

GSM Security:

Security in GSM is implemented through a combination of authentication procedures, encryption mechanisms, temporary identity assignment, and equipment validation. These features are essential to protect subscribers from fraud, prevent unauthorized access, secure user data, and maintain privacy during communication. GSM security is built into both the radio interface and the core network, ensuring that each step, from user registration to call establishment, is performed securely. The GSM security model relies on three fundamental pillars: **subscriber authentication**, **confidentiality through encryption**, and **anonymity through temporary identities**. All of these mechanisms work together within the GSM architecture to create a secure communication environment.



The first major component of GSM security is **subscriber authentication**, which ensures that only legitimate users can access network services. This process is performed using a secret key known as Ki, stored securely in the SIM card and in the Authentication Center (AUC) of the network. When a user attempts to connect to the network, the AUC generates a random challenge (RAND), which is sent to the mobile station. The SIM uses the Ki and the A3 authentication algorithm to compute a Signed Response (SRES), which is sent back to the network. Since the network calculates the expected SRES using the same Ki, it can verify whether the subscriber is genuine. This challenge–response procedure ensures that Ki never leaves the SIM or AUC, making it extremely difficult for attackers to duplicate a user's identity.

Once the subscriber is authenticated, GSM employs **encryption** to maintain confidentiality of the data transmitted over the radio interface. The encryption is performed using the A5 family of algorithms, where a ciphering key (Kc) is derived from Ki and RAND through the A8 algorithm. This key is used by both the BTS and the mobile station to encrypt and decrypt data. Encryption protects voice calls, SMS, and signalling messages from being intercepted by unauthorized parties. Although the encryption applies only between the mobile station and BTS (not end-to-end), it significantly enhances security on the vulnerable radio link. GSM supports several versions of A5, with varying strengths, and operators choose the appropriate one depending on regional security regulations.

Another important aspect of GSM security is **user identity confidentiality**. To prevent attackers from tracking a user by repeatedly listening to the transmission of the permanent identity (IMSI), GSM assigns a Temporary Mobile Subscriber Identity (TMSI). Once the mobile station completes a location update in a new location area, the network issues a TMSI, which replaces the IMSI during most signalling procedures. This temporary identity changes frequently, making it extremely difficult for attackers to trace or identify users. Only in rare cases, such as initial registration, is the IMSI transmitted over the air.

In addition to securing subscribers, GSM also implements **equipment security** using the Equipment Identity Register (EIR). Each mobile device contains an IMEI (International Mobile Equipment Identity), which is checked against the EIR. The EIR maintains three lists: the "white list" for authorized devices, the "black list" for stolen or unauthorized devices, and the "grey list" for devices with suspicious activity. By comparing the IMEI with these lists, the network can block stolen phones, track malfunctioning devices, and prevent illegal equipment from operating.

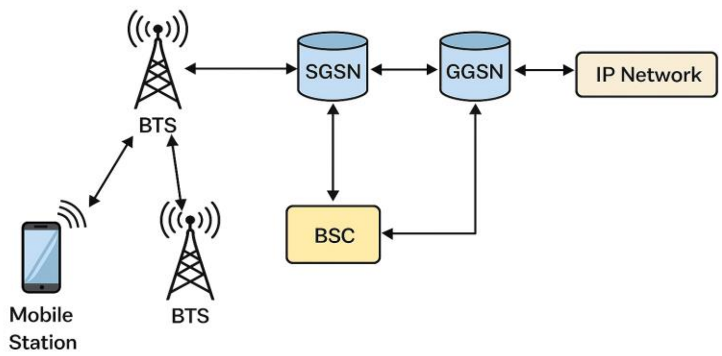
General Packet Radio Service (GPRS)

It is an enhancement to the GSM network that introduces packet-switched data transmission, enabling more efficient and flexible use of radio resources. Unlike GSM, which was originally designed for circuit-switched voice services, GPRS allows multiple users to share the same radio channels simultaneously, making it ideal for applications such as mobile internet browsing, email access, multimedia messaging, and IoT communication. GPRS is often referred to as a 2.5G technology because it bridges the gap between the second-generation GSM systems and third-generation mobile networks.

GPRS works by utilizing unused time slots in the GSM TDMA frame structure. Instead of dedicating a channel to a single user for the entire session (as in circuit switching), GPRS transmits information in packets, allocating radio resources only when data is being sent or received. This makes data communication more efficient, especially for applications that require intermittent transfer, such as browsing or messaging. The use of packet switching also allows multiple users to share the same channel, improving overall network utilization and reducing congestion.

To support packet data transmission, GPRS introduces new network nodes within the existing GSM architecture. The two most important elements are the **Serving GPRS Support Node (SGSN)** and the **Gateway GPRS Support Node (GGSN)**. The SGSN is responsible for mobility management, session management, and packet delivery within the operator's network. It authenticates the user, tracks their location, and forwards data packets between the Base Station Subsystem (BSS) and the GGSN. The GGSN, on the other hand, serves as the interface between the GPRS network and external packet data networks such as the Internet. It allocates IP addresses to mobile devices and routes packets to and from the SGSN.

GPRS Architecture



In addition to new core network elements, GPRS requires upgrades to the radio interface through a component known as the **Packet Control Unit (PCU)**, which may be integrated into the Base Transceiver Station (BTS) or the Base Station Controller (BSC). The PCU manages radio resource allocation for packet data, schedules uplink and downlink transmissions, and handles quality-of-service parameters such as reliability and throughput. GPRS also introduces coding schemes (CS-1 to CS-4) that define how data is protected against errors. Higher coding schemes offer faster data rates but are more vulnerable to interference.

From a user's perspective, GPRS provides several advantages over GSM data services. One key benefit is the concept of "always-on" connectivity, where users can remain connected to the network without occupying resources continuously. This makes services like instant messaging, push email, and online apps more practical. Theoretical GPRS speeds can reach up to 171.2 kbps, although practical speeds are usually lower due to limited time slot availability and network conditions.

GPRS also incorporates mobility features similar to those in GSM. The SGSN maintains the user's packet session as the mobile device moves across cells or location areas. Handover procedures ensure continuity of data transmission, although packet loss can occur in weaker coverage areas. GPRS supports both point-to-point services, such as mobile internet, and point-to-multipoint services, such as broadcast messaging.

Security in GPRS is enhanced compared to GSM due to stronger encryption mechanisms and separate authentication processes performed at the SGSN. GPRS uses the same SIM-based authentication system but employs new ciphering algorithms designed specifically for packet data. However, encryption still occurs only between the mobile station and the SGSN, not across the entire data path.

Features

- Packet-switched technology
- Always-on connectivity
- Dynamic allocation of time slots
- Supports multiple coding schemes (CS-1 to CS-4)
- Integration with GSM network
- IP-based communication
- Uplink and downlink separation
- Mobility support
- Quality of Service (QoS) parameters
- Supports both point-to-point and point-to-multipoint services

Advantages of GPRS

- Higher data speeds
- Efficient spectrum utilization
- Cost-effective for users
- Supports modern applications
- Enhances GSM infrastructure
- Reliable roaming support
- Better network utilization
- Reduced call setup time
- Strong security features

Disadvantages of GPRS

- Lower data speeds compared to modern technologies
- Shared bandwidth
- Higher latency
- Limited time slot availability
- Performance depends heavily on signal quality
- Slow handover process
- No guaranteed Quality of Service (QoS)
- Requires network upgrades
- Encryption applied only between MS and SGSN
- Outdated technology

Applications of GPRS

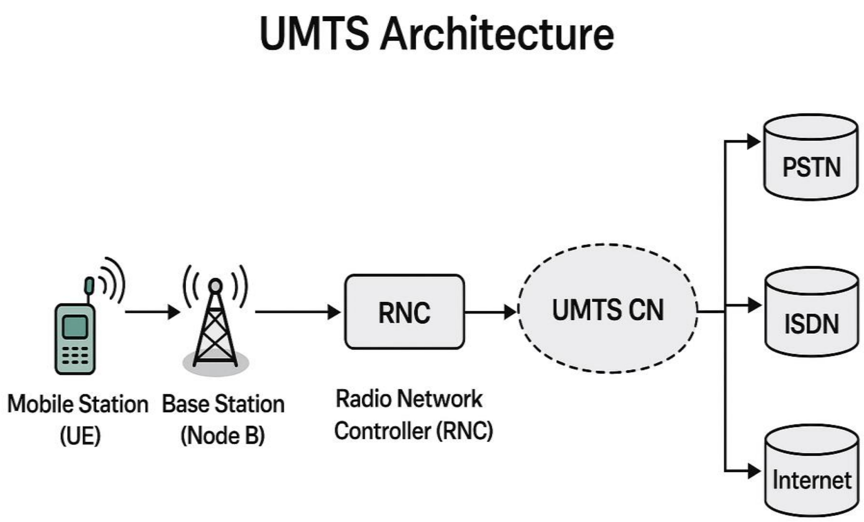
- Mobile Internet browsing
- Email services
- Multimedia Messaging Service (MMS)
- Instant messaging and chat applications
- Location-based services
- Machine-to-Machine (M2M) communication
- Remote monitoring
- Online banking and mobile payment services
- Download/upload of small files
- WAP-based services

Universal Mobile Telecommunications System (UMTS)

Universal Mobile Telecommunications System (UMTS) is a third-generation (3G) mobile communication technology developed by the 3GPP to provide higher data rates, improved spectral efficiency, and support for multimedia services. UMTS represents a major evolution from GSM and GPRS by introducing Wideband Code Division Multiple Access (WCDMA) as its primary air interface. This enables UMTS to offer higher capacity, enhanced quality of service, and support for real-time services such as video calling, mobile TV, and high-speed internet browsing.

UMTS integrates both circuit-switched and packet-switched domains, making it suitable for voice as well as broadband data services. It provides data rates of up to 384 kbps for mobile users and up to 2 Mbps for stationary subscribers. By using wideband radio channels of 5 MHz and advanced spreading codes, UMTS allows multiple users to share the same frequency band efficiently. UMTS networks also adopt all-IP architecture in later releases, paving the way for HSPA (3.5G) and LTE (4G).

UMTS relies on a layered and modular architecture that separates the radio access network from the core network. This separation allows flexible deployment strategies and simplifies upgrades when new technologies such as HSPA and LTE are introduced. The core network of UMTS supports mobility management, call/session control, authentication, and interworking with external networks. UMTS is also backward compatible with GSM, allowing seamless roaming and sustained global connectivity.



UMTS Architecture

The UMTS architecture consists of three major components:

1. User Equipment (UE)
2. UMTS Terrestrial Radio Access Network (UTRAN)
3. Core Network (CN)

1. User Equipment (UE)

The UE is the subscriber's mobile device, which includes a handset, software, and a Universal Subscriber Identity Module (USIM). The USIM stores authentication information, encryption keys, subscriber identity, and user profiles. The UE communicates with the UTRAN through the WCDMA interface (Uu interface). It supports features such as mobility management, radio resource control (RRC), signal measurement, and handovers between cells.

2. UMTS Terrestrial Radio Access Network (UTRAN)

The UTRAN is responsible for all radio-related functions and forms the bridge between the UE and the Core Network. It consists of:

a. Node B (Base Station)

Node B is the equivalent of the BTS in GSM. It handles modulation, coding, spreading, and RF transmission. It supports soft handovers, one of the key advantages of WCDMA, allowing the UE to remain connected to multiple cells simultaneously, improving reliability and signal quality.

b. Radio Network Controller (RNC)

The RNC is similar to the BSC in GSM but with more advanced functions. It controls multiple Node Bs and handles functions such as:

- Radio Resource Management (RRM)
- Handover control (intra- and inter-RNC)
- Power control

- Load control
- Admission control
- Ciphering and integrity protection
- Mapping of data streams to transport channels

The RNC also interfaces with the Core Network through two domains: **Circuit-Switched (CS)** and **Packet-Switched (PS)**.

UTRAN uses the **Iub** interface between RNC and Node B, **Iur** between RNCs, and **Uu** for UE-to-Node B communication.

3. Core Network (CN)

The UMTS Core Network is built on the GSM core but enhanced for high-speed packet data. It has two major domains:

a. Circuit-Switched (CS) Domain

Handles traditional voice calls.

Main elements:

- **MSC** (Mobile Switching Center)
- **GMSC** (Gateway MSC)

These nodes perform call routing, mobility management, and interconnection with PSTN/ISDN.

b. Packet-Switched (PS) Domain

Handles internet data and packet services.

Main elements:

- **SGSN** (Serving GPRS Support Node)
- **GGSN** (Gateway GPRS Support Node)

The SGSN tracks subscriber mobility, performs authentication, and forwards packet data.

The GGSN interfaces with external IP networks and assigns IP addresses to UEs.

c. Databases

- **HLR** (Home Location Register)
- **VLR** (Visitor Location Register)
- **AuC** (Authentication Center)
- **EIR** (Equipment Identity Register)

These databases store subscriber profiles, security keys, and equipment identifiers.

UMTS Features:

- WCDMA Air Interface
- High data speeds
- Support for multimedia services
- Soft handover capability
- Enhanced spectral efficiency
- Flexible QoS (Quality of Service)
- Seamless integration with GSM/GPRS
- All-IP evolution path
- Advanced power control
- Support for circuit-switched and packet-switched services
- Improved security

Advantages of UMTS

- Much higher data rates
- Supports simultaneous voice and data
- Superior multimedia experience

- Soft handover reduces call drops
- High network capacity
- Better QoS control
- Smooth evolution to 3.5G and 4G
- Global roaming support
- Stronger authentication and encryption
- Efficient use of spectrum

Disadvantages of UMTS

- High infrastructure cost
- Requires wider bandwidth (5 MHz)
- Higher power consumption
- Network deployment challenges
- Interference management complexity
- Lower battery life
- Slower initial data rates
- Backward compatibility limitations
- Soft handover requires careful coordination
- Competition from faster technologies

Comparison of GSM, GPRS, UMTS and LTE

Feature	GSM	GPRS	UMTS	LTE
Full Form	Global System for Mobile Communications	General Packet Radio Service	Universal Mobile Telecommunications System	Long-Term Evolution
Generation	2G	2.5G	3G	4G
Technology Type	Circuit-switched	Packet-switched overlay on GSM	WCDMA (Wideband CDMA)	OFDMA (DL) & SC-FDMA (UL)
Channel Bandwidth	200 kHz	200 kHz (shared for packet data)	5 MHz	1.4–20 MHz
Data Rate	Up to 9.6–14.4 kbps	30–80 kbps (theoretical 171 kbps)	384 kbps to 2 Mbps	50–150 Mbps DL, 10–50 Mbps UL

Core Network	Circuit-switched	CS + PS (SGSN/GGSN added)	CS + PS (Evolved RNC, SGSN/GGSN)	All-IP EPC (MME, SGW, PGW)
Air Interface	FDMA/TDMA	Same as GSM	WCDMA	OFDMA/SC-FDMA
Primary Services	Voice, SMS	Packet data (Internet)	Voice, video call, data, multimedia	High-speed broadband data, VoLTE
Handover Type	Hard	Hard	Soft + Hard	Hard
Latency	High	Medium high	Lower	Very low
Spectral Efficiency	Low	Medium	High	Very high
Mobility Support	Basic mobility	Cell & routing mobility	Fast mobility with soft handover	High-speed mobility up to 350 km/h
Security	Basic encryption (A5)	Improved ciphering	Strong authentication & integrity	Advanced AES/Snow3G encryption
Architecture Complexity	Low	Moderate	High	Very high but simplified (flat architecture)
Applications	Voice/SMS	Early Internet, WAP, MMS	Video calling, mobile Internet, streaming	HD video, VoLTE, online gaming, IoT, broadband